

### DRAWING AMENDMENTS

The Applicant respectfully requests approval of the amendment to Figure 1 as depicted in the Appendix accompanying this paper. Appendix A includes both a red line version of Figure 1, which is labeled “Annotated Sheet Showing Changes,” as well as a new drawing sheet that is labeled “Replacement Sheet” and which includes the amended figure.

The proposed change to FIG. 1 is to add the legend –Prior Art— as required in the Final Office Action. No new matter is introduced.

## **REMARKS**

### **DRAWINGS**

In amended Figure 1, the legend --Prior Art-- has been added as required by the Final Office Action. The Applicant respectfully submits that the amendment of Figure 1 traverses the objection to the drawings.

### **STATUS OF CLAIMS**

Claims 1, 3, 4, 7, 9, 11, 13, 16, 18, 19, 22, 24, 26, 27, 30, 31, 33, 34, 38, and 39 have been amended.

No claims have been cancelled, added, or withdrawn.

Claims 1-41 are currently pending in the application.

### **INTERVIEW SUMMARY**

The Applicant thanks the Examiner for the in-person Interview conducted on December 14, 2004. The interview was between Examiner Jacob Lipman, Primary Examiner Gilberto Barron, and the applicant's attorney, Christopher J. Palermo. During the interview, the 112 issues, prior art label for FIG. 1, and the inventor's address were discussed. The Applicant raised the issue of the entry and examination of Claims 32-41 provided in the response to the first Office Action. The Examiner agreed to reconsider the arguments and whether to remove the finality of the Office Action dated November 16, 2004, upon the receipt of this response. However, no agreement was reached as to the allowability of the claims. The Applicant is providing herein the claim amendment that was proposed during the interview.

### **SUMMARY OF THE REJECTIONS/OBJECTIONS**

The Oath/Declaration has been objected to as allegedly failing to provide the inventor's post office address. The drawings have been objected to because FIG. 1 allegedly only illustrates that which is old and is not identified as --Prior Art--. Claims 3, 4, 9, 11, 18, 19, 22, 26, and 27 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claims the subject matter

which applicant regards as the invention. Claims 1-31 have been rejected under 35 U.S.C. § 102(b) as allegedly anticipated by “the admitted prior art,” or, in the alternative, under 35 U.S.C. 103(a) as obvious over the “admitted prior art.” The rejections are respectfully traversed.

## RESPONSE TO REJECTIONS NOT BASED ON THE PRIOR ART

### A. OATH/DECLARATION & “POST OFFICE ADDRESS”

Accompanying the previously filed Response to Final Office Action was a supplemental Application Data Sheet (ADS) for the present application. According to 37 CFR 1.76(c)(1-2) and MPEP §601.15, a supplemental ADS can be filed to update information in a previously submitted oath or declaration. The previously filed supplemental ADS provides a post office address for inventor Floryanzia, as required by the Final Office Action. Therefore, the Applicant respectfully submits that the previous submission of the supplemental ADS traverses the objection to the oath/declaration in the Final Office Action.

### B. DRAWINGS - LABELING FIG. 1 AS “PRIOR ART”

The drawings have been objected to in the Office Action, and in particular, the Office Action alleges that “Figure 1 should be designated by a legend such as -- Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).” As part of this response, a drawing amendment is included to add the legend –PRIOR ART—as required by the Final Office Action. Therefore, the Applicant respectfully submits the amendment to FIG. 1 traverses the objection to the drawings.

### C. INDEFINITENESS REJECTIONS

Claims 3, 4, 9, 11, 18, 19, 22, 26, and 27 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, Claims 4, 9, 19, 22, and 27 have been rejected as being allegedly indefinite for reciting the term “acceptable interval,” and Claims 3, 11, 18, and 26 have been rejected as being allegedly indefinite for reciting the term “H.235 ClearToken.”

Claims 4, 9, 19, 22, 27, 34, and 39 have been amended to replace “an acceptable interval” with “a specified interval.” The use of “specified” in place of “reasonable” makes clear that the interval of time during which the authentication request information was created with respect to the current time is a specified interval of time. The actual value of the specified interval depends on the particular circumstances of a particular implementation. As described in the examples in the application, in one embodiment, the specified interval of time is about 30 seconds (e.g., *see* page 16, line 24 through page 17, line 7; page 19, lines 16-21; and page 23, lines 7-12). No new matter is introduced.

Claims 3, 11, 18, 26, 33, and 38 have been amended to replace “an H.235 ClearToken” with “data.” As a result, Claims 3, 11, 18, and 26 recite “receiving data comprising a general identifier value, a time stamp value, a challenge value, and a random value,” thereby eliminating the use of any terminology that could be construed as a trademark or trade name. As described in the application, an H.235 ClearToken is an example of a data structure that carries unencrypted data, which can be referred to more generally as “data.” (See application, page 11, lines 10-15.) No new matter is introduced.

The Applicant respectfully submits that the amendments to Claims 3, 4, 9, 11, 18, 19, 22, 26, 27, 33, 34, 38, and 39 traverse the rejections under 35 U.S.C. § 112, second paragraph.

#### RESPONSE TO REJECTIONS BASED ON THE PRIOR ART

Claims 1-31 have been rejected under 35 U.S.C. § 102(b) as allegedly anticipated by “the admitted prior art,” or, in the alternative, under 35 U.S.C. 103(a) as obvious over the “admitted prior art.” The rejections are respectfully traversed.

##### A. INTRODUCTION TO CLAIM 1

As amended above, Claim 1 features:

“A method of securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, the method comprising the computer-implemented steps of:  
receiving **non-encrypted authentication request information that includes challenge information** from the first node;

receiving, from an **authentication server** that is **separate from but** communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information **and including challenge response information generated by the authentication server;** and  
establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.” (Emphasis added.)

Thus, Claim 1 features the use of an authentication server that is separate from yet communicatively coupled to the second node. The authentication server, not the second node, authenticates the first node based on the non-encrypted authentication request information that includes challenge information and that is received from the first node, and the authentication server generates challenge response information instead of the second node. The call between the first node and second node is only established when the authentication message indicates that the first node is authenticated at the authentication server based on the challenge response information generated by the authentication sever. The challenge response information is generated by the authentication server in response to the challenge information that is included in the non-encrypted authentication request information.

Because of the use of non-encrypted authentication request information in the approach of Claim 1, there is no need for an authenticating gatekeeper to maintain or acquire passwords for users and gateways. (See Application, page 11, lines 10-15.) For example, while the H.235 recommendation relies upon CryptoTokens that include encrypted information (Application, page 4, lines 1-15) that would require the gatekeepers to track a potentially large number of gateway ID’s and passwords (Application, page 4, lines 16-26), the approach of Claim 1 relies upon non-encrypted authentication request information, such as ClearTokens that are data structures that carry unencrypted data (Application, page 11, lines 10-15).

While the use of the non-encrypted authentication request information may impact the security provided in the conventional H.235 approach, the use of an authentication server in the approach of Claim 1 provides security in lieu of using encrypted authentication request

information. Specifically, in the approach of Claim 1, the authentication server authenticates the first node based on the non-encrypted authentication request information, and an authentication messages is received from the authentication server that indicates whether the first node is authenticated or not. Thus, while in the conventional H.235 approach security is provided by the gatekeeper that performs authentication, in the approach of Claim 1, the burden of authenticating the first node is born by the authentication server, which is a mechanism that is designed specifically for performing an authentication function.

#### B. EXAMPLE OF CLAIM 1 WITH REFERENCE TO FIGURES 1, 2, AND 3

In the prior approach illustrated in FIG. 1 of the present application, the receiving node, such as Gatekeeper 102B, performs authentication of the sending node, such as Gateway 110, using encrypted information that includes a shared secret (e.g., a password) that is sent from the sending node to the receiving node. As a result, the receiving node has to maintain a global database of passwords from all possible sending nodes in order to authenticate any potential sending node, or the receiving node must contact such a global database that is located elsewhere, possibly using insecure communication links.

However, in the approach of Claim 1, as illustrated in the embodiment depicted in FIG. 2 of the present application, a third party or entity, such as an authentication server 202, is used in the system for performing authentication, and thus the system includes an authentication server that is separate from the sending and receiving nodes. As a specific example, authentication server 202 is communicatively coupled to an authentication database 206, thereby relieving the receiving node of either the burden of maintaining its own global database of passwords for all possible sending nodes or the need to contact such a global database that is located elsewhere, possibly over insecure communication links.

Furthermore, the use of authentication server 202 with authentication database 206 allows the sending node, such as Gateway 110, to send unencrypted information, such as by using an access token 204 that includes challenge information. (See FIG. 2B, illustrating that access token 204 includes a challenge value 214.) Based on the unencrypted information in the form of access token 204, authentication server 202 can generate challenge response information that is compared to the challenge information from access token 204. Based upon

the comparison, the sending node is either authenticated (so that the call is put through) or not authenticated (resulting in denial of the call).

FIGs. 3A, 3B, and 3C provide a more detailed example of an embodiment of Claim 1, with the various steps performed by the gateway, the gatekeeper, and the authentication server grouped under the proper header for each device in the interactions. For example, in FIG. 3A, the gateway generates the access token (step 302), creates the registration request (RRQ) message that includes the access token (step 304), and sends the RRQ message to the gatekeeper (step 306). The gatekeeper then determines whether the access token is timely (step 308), and if not, the message is discarded (step 310), but if so, the gatekeeper continues to format an access request packet (step 312) that is then sent to the authentication server (step 314).

The authentication server, using the unencrypted information in the form of the access token that is included in the access request packet, locates a password (e.g., in authentication database 206) that is associated with an alias of the gateway (step 320). Then the authentication server generates a challenge response (such as by using the CHAP protocol) using the alias, the password, and the challenge information from the gatekeeper (step 322). If the challenge response information matches the challenge request information/attributes (step 324), then the authentication server sends an access accept packet to the gatekeeper (step 326). If the challenge response information does not match the challenge request, then the authentication server send an access reject packet to the gatekeeper (step 328).

If the gatekeeper receives an access accept packet (step 330), the gatekeeper responds to the gateway with a registration confirm (RCF) message (step 332). If the gatekeeper receives an access reject packet (step 334), the gatekeeper responds to the gateway with a Registration Reject (RRJ) message (step 336).

The key points to note in the embodiment of Claim 1 illustrated in FIGs. 3A, 3B, and 3C is that a third player, namely the authentication server, is involved in handling the challenge and challenge response steps that otherwise would be performed by the receiving node. As a result, the receiving node need not maintain a global database of passwords of all possible sending nodes or have to contact such a global database, such as by using insecure links. Furthermore, the authentication request information need not be encrypted in the approach of Claim 1 as illustrated in the embodiment of FIGs. 3A, 3B, and 3C, which is in

contrast to the normal H.235 approach in which the authentication request information is encrypted.

### C. REFERENCES PROVIDED WITH THE FINAL OFFICE ACTION

The Notice of References Cited Form PTO-892 accompanying the Final Office Action lists two references from Cisco's website, which are referred to at the end of the Detailed Action. The first reference listed on the PTO-892 form, titled "Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide," has a publication date of December 2, 2003, which can be seen in the footer of the PDF version of the online document when printed. The PDF version of this reference can be accessed at the URL listed on the PTO-892 form by clicking on the PDF icon on the upper right corner at the beginning of the HTML document. Unfortunately, the publication date does not appear in the footer of the HTML version of the document when printed (a copy of which was provided with the Final Office Action.) For the Examiner's convenience, a copy of the PDF version's first page of this reference is provided in Appendix B from which it can be verified that the publication date is "12/2/2003." Because the filing date of the application is September 28, 2000, which is well before the publication date of the first reference of December 2, 2003, the Applicant respectfully submits that this first reference does not qualify as prior art against the present application.

The second reference listed on the PTO-892 form, titled "Cisco H.323 Gateway Security and Accounting Enhancements," merely describes prior approaches such as those discussed in the Background section of the application in which authentication is performed by the receiving node based on encrypted information, which is in contrast to the approach of Claim 1 in which authentication is performed by the authentication server based on non-encrypted information.

Specifically, on page 5, step 11 of the second reference, Gatekeeper B (e.g., the receiving node) in the second reference validates the authentication information in the access token (e.g., the encrypted information that is sent by Gatekeeper A, the sending node) that is sent in step 8 on page 11. (Note that page references for the second reference are based on the PDF version of the document, which can be accessed via the PDF link at the top right of the HTML version of the online document.)



D. CONCLUSION OF DISCUSSION OF CLAIM 1

Because the “admitted prior art” does not disclose, teach, suggest, or in any way renders obvious “receiving **non-encrypted authentication request information that includes challenge information** from the first node” and “receiving, from an **authentication server** that is **separate from but** communicatively coupled to the second node, an authentication message indicating **whether the first node is authenticated based on the non-encrypted authentication request information and including challenge response information generated by the authentication server,**” the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

E. CLAIMS 7, 16, 24, 30, AND 31

Claims 7, 16, 24, 30, and 31 contain features that are either identical or similar to those described above with respect to Claim 1. In particular, Claim 7 features “an authentication server that is separate from but communicatively couple to the first gatekeeper and the second gatekeeper,” “non-encrypted authentication request information that includes challenge information,” “receiving non-encrypted authentication request information from the first gateway,” and “receiving from the authentication server an authentication message that includes challenge response information generated by the authentication server and indicating whether the first gateway is authenticated based on the non-encrypted authentication request information,” all of which are nearly the same as in Claim 1.

Similarly, Claim 16 features “an authentication server that is separate from but communicatively couple to the first gatekeeper and the second gatekeeper,” “non-encrypted authentication request information that includes challenge information,” “receiving non-encrypted authentication request information that includes challenge information from the first gateway,” and “receiving from the authentication server a second authentication message indicating whether the first gateway is authenticated based on the non-encrypted authentication request information and second challenge response information generated by the authentication server”, which again are nearly the same as in Claim 1.

Finally, Claims 24, 30, and 31 all feature “receiving non-encrypted authentication request information that includes challenge information from the first node” and “receiving,

from an authentication server that is separate from but communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information and challenge response information generated by the authentication server,” which are the same as in Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 7, 16, 24, 30, and 31 are allowable over the art of record and are in condition for allowance.

F. CLAIMS 2-6, 8-15, 17-23, 25-29, 32-36, AND 37-41

Claims 2-6, 8-15, 17-23, 25-29, 32-36, and 37-41 are dependent upon Claims 1, 7, 16, 24, 30, and 31, respectively, and thus include each and every feature of the corresponding independent claims. Each of Claims 2-6, 8-15, 17-23, 25-29, 32-36, and 37-41 is therefore allowable for the reasons given above for the Claims 1, 7, 16, 24, 30, and 31. In addition, each of Claims 2-6, 8-15, 17-23, 25-29, 32-36, and 37-41 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2-6, 8-15, 17-23, 25-29, 32-36, and 37-41 are allowable for the reasons given above with respect to Claims 1, 7, 16, 24, 30, and 31.

CONCLUSION

The Applicant believes that all issues raised in the Final Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

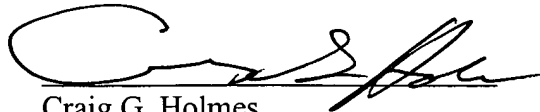
For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP



Craig G. Holmes  
Reg. No. 44,770

**Date: March 25, 2005**

2055 Gateway Place, Suite 550  
San Jose, California 95110-1089  
Telephone: (408) 414-1080, ext. 207  
Facsimile: (408) 414-1076

Appendix A  
Appendix B

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop RCE, P.O. Box 1450, Alexandria, VA 22313-1450.

on March 25, 2005 by Tracy Reynolds

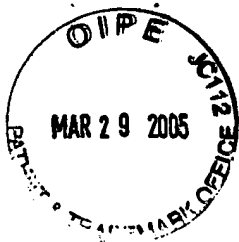


**Appendix A –**

**Drawing Amendment**  
**for Figure 1**

**(Annotated Sheet Showing Changes)**

**(Replacement Sheet)**

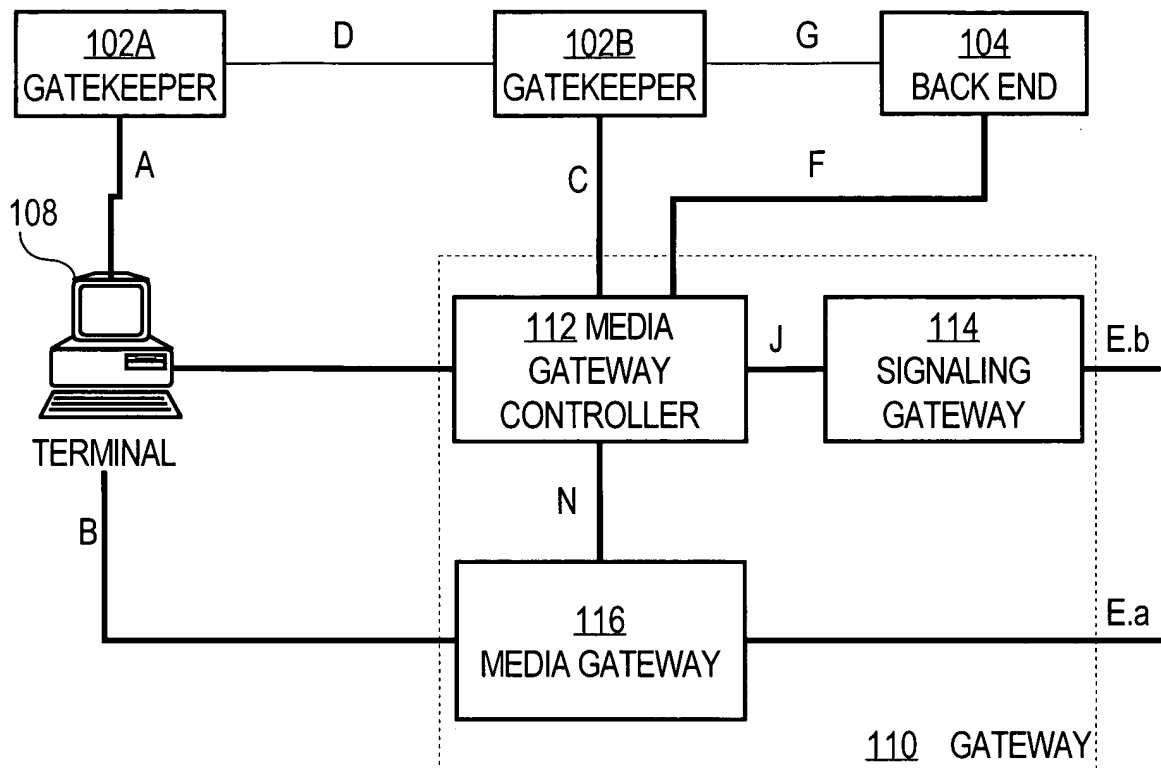


ANNOTATED SHEET SHOWING CHANGES

Title: Authenticating Endpoints of a Voice  
Over Internet Protocol Call Connection  
Inventor: Tyrone Floryanzia  
Serial No.: 09/676,265  
Docket No. 50325-0102

**FIG. 1**

*PRIOR ART*





## **Appendix B –**

**Copy of First Page of PDF Version of First  
Reference Listed on PTO-892 Form  
Accompanying Final Office Action Showing  
Publication Date of 12/2/2003**

MAR 29 2005

# Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide

## Contents

### Introduction

#### Intradomain Gateway to Gatekeeper Security

[Time Stamp Passed in the Tokens](#)[How Cisco Implements the H.235 Recommendation](#)[How to Configure the Security Levels](#)[H.235 Usage on a Per-call Level without IVR](#)[Major Issues](#)[Debugs and Call Flow for the Different Levels](#)[Gateway IOS Problem](#)[Security with Alternate Endpoints](#)[OSP Token Support](#)[Different Levels of Security for each Endpoint or Zone](#)

#### Interdomain Gatekeeper to Gatekeeper Security

[Implementing Gatekeeper to Gatekeeper Security](#)[Gatekeeper Configuration](#)[IZCT Call Flow](#)[Call Flow with Debugs](#)

### Related Information

## Introduction

H.323 networks have different kinds of configurations and call flows. This document attempts to document most of the the security concerns with H.323 networks that involve gatekeepers. This document summarizes the way each feature works and how to troubleshoot it with an explanation to most of the debugs. This document does not address the overall security of Voice over Internet Protocol (VoIP).

This document covers the following features:

- **Intradomain Gateway to Gatekeeper Security** This security is based on H.235, in which H.323 calls are authenticated, authorized, and routed by a gatekeeper. The gatekeeper is considered a known and trusted entity in a sense that the gateway does not authenticate it when the gateway tries to register with it.
- **Interdomain Gatekeeper to Gatekeeper Security** This security covers authenticating and authorizing of H.323 calls between the administrative domains of Internet Telephone Service Providers (ITSPs) using InterZone Clear Token (IZCT). This document covers only the portion where the terminating gatekeeper sends a token in its location confirmation (LCF) message so that it authenticates the answerCall Admission Request (ARQ). Location request (LRQ) validation is not included in this feature. LRQ validation is a feature scheduled for a future Cisco IOS release.

### Definitions

Acronym	Definition
ARQ	Admission Request A RAS message sent from an H.323 endpoint to a gatekeeper requesting an admission to establish a call.